REMARKS

The application has been amended and is believed to be in condition for allowance.

This amendment is being filed as part of an RCE application.

Applicant appreciates Examiner Henning's time and cooperation in arranging and conducting the interview of October 27, 2006, as well as his helpful critique and suggestions.

The previously pending claims have been replaced with new claims that take into account the criticisms of the Official Action. The same invention is being recited and therefore an RCE application is appropriate.

The claims find support in the specification as originally filed and drawing Figures 1-5. See particularly beginning with specification page 6, line 21. Reference numbers are included in the claims as a convenience but do not in any way limit the claims.

There are no formal matters outstanding.

Claims 9-16 stand rejected as obvious over FRANCISCO et al. 5,263,147 in further view of CLIFTON 5,469,556.

The applied references do not, individually or in combination, teach or suggest the invention's recited combination of features.

Neither FRANCISCO nor CLIFTON teaches or suggests the recited system with two different processors (a computer

processor and a security device processor), where the security device processor (52) includes a protection mode signal generator (SGpm) and an alter signal generator (SGa), and further comprising a switch (60) connected to each handling device (e.g., memory), the switch containing a table (T) of addresses to different ones of the handling devices and a comparator (C), the table having accessibility allocations specifying handling devices allocated only to the security device and the table specifying handling devices allocated to the computer processor operating in a normal mode, the switch being changeable only under control of signals generated by the security device.

Neither FRANCISCO nor CLIFTON teaches or suggests the recited alter signal receiver (SRa), source signal receiver (SRs), and protection mode signal receiver (SRpm) connected to the switch where the switch is connected to address lines and to operation lines of the bus.

Neither FRANCISCO nor CLIFTON teaches or suggests that the switch is configured for i) a first normal mode wherein the computer processor has access to a first group of the handling devices, and ii) a second protected mode wherein the computer processor is denied access to the first group of handling devices and the security processor is allowed access to the first group of handling devices and to execute a security critical activity with the first group of handling devices, and said signals from the security device, enabling the security device and the

security processor access to the handling devices and denying the computer processor access to the handling devices, changes the switches from the first normal mode into the second protection mode.

Thus, independent claim 22 is believed patentable.

Neither FRANCISCO nor CLIFTON teaches or suggests (as per claim 23) that to enter the secure management mode, i) the protection mode signal generator issues a request signal to the protection mode signal receiver, and ii) based on information in the table, access by the computer processor to the handling devices is withdrawn and access to the handling devices is solely limited to the security device processor.

Neither FRANCISCO nor CLIFTON teaches or suggests (as per claim 24) a director (68) connected to the switch and connected to each handling device, wherein, the director is connected to the address lines and to the operation lines of the bus.

Neither FRANCISCO nor CLIFTON teaches or suggests (as per claim 25) that each switch further comprises an enable-abort line (66), and the director (68) is connected to the switch via the enable-abort line.

Neither FRANCISCO nor CLIFTON teaches or suggests (as per claim 26) that only the security device can change contents of the table, the security device configured so that the alter

signal generator sends an alter signal to the alter signal receiver to alter the contents of the table.

Neither FRANCISCO nor CLIFTON teaches or suggests (as per claim 27) that the handling device comprises a first part of the main memory and a second part of the main memory, with one of the switches connected between the first and second parts of the main memory and the bridge, so that

- in the normal mode, the contents of the table allows access to the first part of the main memory to the security device processor and allows access to the second part of the main memory to the computer processor, and

- in the secure management mode, the contents of the table allows access to the first and second parts of the main memory to only the security device processor.

Neither FRANCISCO nor CLIFTON teaches or suggests (as per claim 28) that the one switch further controls access to the second part of the main memory based a source making the access request.

Neither FRANCISCO nor CLIFTON teaches or suggests (as per claim 29) that the handling device comprises a screen controller of a monitor, one of the switches is connected between the screen controller and the bridge, so that

- in the normal mode, the contents of the table allows the computer processor full access, via the controller, to the monitor, and

- in the secure management mode, the contents of the table denies the computer processor complete access to the monitor and allows the security device processor access to a part of the monitor denied to the computer processor.

Neither FRANCISCO nor CLIFTON teaches or suggests (as per claim 30), when taken in combination with the other claim recitations, that each handling device is one of a part of the main memory (16, 74), a hard disk (42), a keyboard (32), a monitor (20), a card slot (28), a mouse (36), floppy drive (34), and a smart card reader (38).

Neither FRANCISCO nor CLIFTON teaches or suggests (as per claim 31), when taken in combination with the other claim recitations, the bridge is one of a Host-PCI bridge (14) and a E-ISA bridge (24).

Neither FRANCISCO nor CLIFTON teaches or suggests (as per claim 32), the security device processor is configured to i) run the normal mode with access to a second group of the handling devices, and ii) run the security critical activity in the secure management mode with access to both the first and second groups of the handling devices, and the switch is configured to control access to each handling device by the comparator checking an access request from the computer processor and the security device processor with the accessibility allocations in the table, a positive checking result by the

comparator directing data and operation signals to and from the accessed handling device.

Claim 33 is also independent. Neither FRANCISCO nor CLIFTON teaches or suggests the combination of

- a security device (50) comprising a security device processor (52) with a protection mode signal generator (SGpm), the security device processor connected to the bridge;

- a switch (60) connected between the bridge and the main memory, the switch containing an information table (T) and a comparator (C), the table having accessibility allocations specifying parts of the maim memory allocated only to the security device and other parts of the main memory allocated to the computer processor operating in a normal mode, and

- the switch being operative only under control of signals generated by the security device.

Neither FRANCISCO nor CLIFTON teaches or suggests the further recited features of signal receivers connected to the switch, wherein, the switch is connected to address lines and to operation lines of the computer.

Neither FRANCISCO nor CLIFTON teaches or suggests the further recited features of the computer being configured to run in the normal mode with the computer processor having access to a first part of the main memory and the security device processor configured to i) run the normal mode with access to a second part of the main memory, and ii) run a security critical activity in a

secure management mode with access to both the first and second parts of the main memory while the computer processor is denied access to the first part of the main memory.

Neither FRANCISCO nor CLIFTON teaches or suggests the further recited features of the switch configured to control access to each part of the maim memory by the comparator checking an access request from the computer processor and the security device processor with the accessibility allocations in the table, a positive checking result by the comparator directing data and operation signals to and from the accessed parts of the main memory.

Therefore, this claim is also believed patentable.

Neither FRANCISCO nor CLIFTON teaches or suggests the recited features of independent claim 36, i.e., in a computer comprising a connecting element (14) connecting the computer processor to the main memory and a security device processor connected by the bridge to the main memory, there being:

- a switch (60) connected between the connecting element and the main memory, the switch containing a table (T) and a comparator (C), the table having accessibility allocations for the security device and for the computer processor operating,

- the switch being operative only under control of signals generated by the security device; and

- an alter signal receiver (SRa), a source signal receiver (SRs), and a protection mode signal receiver (SRpm) connected to the switch, wherein,

the switch is connected to address lines and to operation lines of the bus,

the switch is configured for i) a first normal mode wherein the computer processor has access to a first part of the main memory, and ii) a second protected mode wherein the computer processor is denied access to the first part of the main memory and the security processor is allowed access to the first part of the main memory to execute a security critical activity with the first part of the main memory.

Neither FRANCISCO nor CLIFTON teaches or suggests the recited features as per claim 37, wherein, the switch is configured to control access to each part of the main memory by the comparator checking an access request from the computer processor and the security device processor with the accessibility allocations in the table, a positive checking result by the comparator directing data and operation signals to and from the accessed handling device.

Therefore, these claims are also believed patentable.

Accordingly, reconsideration and allowance of all the pending claims are respectfully requested.

The Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any

overpayment to Deposit Account No. 25-0120 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17.

Respectfully submitted,

YOUNG & THOMPSON

Roland E. Long, Jr., Reg. No. 41,949
745 South 23rd Street
Arlington, VA 22202
Telephone (703) 521-2297
Telefax (703) 685-0573
(703) 979-4709

REL/lrs